Oslo, 12. april 2010

Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

Deres ref. 09/585-HK

Høring om datalagring

Vi henviser til høringsnotatet utarbeidet av Samferdselsdepartementet, Justisdepartementet og Fornyings-, administrasjons- og kirkedepartementet angående innlemmelse av EUs Datalagringsdirektiv (DLD) i EØS-avtalen.

Prinsipielt spørsmål

Vi vil i denne høringsuttalelsen legge vekt på de prinsipielle spørsmålene i forbindelse med den potensielle innføringen av datalagringsdirektivet i Norge. Vi står nå foran et veiskille der begrensningene på innsamlingen av data om landets borgere ikke lenger er gitt av dataenes tilgjengelighet og ressursene man har til rådighet, men av hvor vi selv setter grensene.

Tidligere var etterforskning og innsamling av data begrenset av hva som ble lagret til praktiske formål. Lagring utover praktiske formål var svært ressurskrevende og mer synlig i samfunnet. Derfor har man tradisjonelt kun lagret data utover praktiske formål i de tilfeller der det har vært iverksatt etterforskning i forbindelse med lovbrudd.

I nyere tid har dette endret seg. Med dagens teknologi er loggføring av kommunikasjon allerede en del av de fleste telesystemer. Begrensningen på lagringstid har svært lite med ressurser å gjøre da dagens lagringsteknologi er svært billig, og i fremtiden vil bli enda billigere. Den har i stedet med tillatelse å gjøre. Teleoperatører har i dag ikke lov til å lagre informasjonen lenger enn det som er nødvendig for deres daglige drift.

Spørsmålet vi må stille oss i forbindelse med implementeringen av EUs Datalagringsdirektiv (heretter DLD) er om det er ønskelig å utvide lagringstiden og omfanget av lagringen for kriminalitetsforebyggende og -oppklarende arbeid.

Vi i FriBit mener det er galt å innføre DLD til dette formålet. I det følgende vil vi forklare hvorfor. Som

følge av at vi går mot innføringen av direktivet vil vi ikke gå inn på spørsmålene stilt i høringsnotatet som tar utgangspunkt i at direktivet innføres.

Uskyldig til det motsatte er bevist

Rettsstaten vår bygger på prinsippet om at man er uskyldig til det motsatte er bevist. I dette ligger at man heller ikke skal etterforskes med mindre man er mistenkt for å planlegge, medvirke til eller ha begått en kriminell handling. Prinsippet om uskyldspresumpsjon står sterkt både i borgernes rettsoppfatning og i Europas Menneskerettighetskonvensjon[1].

Innføringen av DLD vil føre til en innsamling av data om alle landets borgere uten å ta hensyn til hvorvidt de er mistenkte eller ikke. Det å snu rundt på uskyldspresumpsjonen vil føre til en rekke uheldige konsekvenser, deriblant en endring av folks atferdsmønster (chilling effect), en forskjøvet balanse mellom det offentlige og private, samt en bevegelse mot en nasjon basert på mistillit framfor tillit – der man må bevise sin uskyld ved enhver korsvei.

Samfunnets informasjonstilgang

I dagens samfunn blir den tilgjengelige informasjonen om hver enkelt borger stadig større. Vi legger igjen spor overalt, og disse sporene blir oftere og oftere tilgjengelige både for påtalemyndigheter og andre medborgere. For hver utvidelse av den tilgjengelige informasjonen blir det lettere å danne et større bilde om hver enkelt borger.

Av hensyn til hver enkelt persons privatliv og personvernet forøvrig bør vi derfor være særs forsiktige med å innføre nye tiltak som utvider informasjonstilgangen. Privatlivet og et tilstrekkelig vern av personlig integritet er nødvendig for menneskers utvikling, og ikke minst for balansen i samfunnet. Det må være anledning til å foreta seg lovlige handlinger i det offentlige (og private) rom uten nøye avveining for om handlingen kan bli brukt mot en i fremtiden. Uten denne anledningen vil samfunnets og borgernes utvikling stagnere. Man bør merke seg at lovlige handlinger ikke alltid tåler dagens lys. Eksempelvis kan man nevne homofili, politisk tilhørighet, legebesøk og psykiatrisk behandling.

Det bør i denne sammenhengen også nevnes at de enorme mengdene informasjon som finnes om enhver borger i samfunnet i dag allerede er problematisk. Behovet for bedre håndtering av disse dataene er sterkt tilstede, men at det er svakheter i dagens datalagring bør ikke være et argument for å utvide lagringen gjennom DLD. Selv om enkelte argumenterer for at DLD vil gi en sterkere kontroll over dataene som lagres, er det viktig å forstå at dette kan gjøres uten å implementere direktivet.

«Chilling Effect»

Begrepet Chilling Effect viser til den selvsensurerende effekten overvåkning har på privat kommunikasjon. Det er tilstrekkelig at personer tror de *kan* bli overvåket, for at de skal endre adferd. En undersøkelse gjort i Tyskland etter innføringen av DLD viser at 11 % av respondentene allerede har unnlatt å ta telefonsamtaler, mens hele 52 % svarte at de ville unnlate å benytte telefon eller epost for konfidensielle henvendelser[2] . Datalagringsdirektivet vil medføre en betydelig innskrenkning i allmennhetens anledning til fri ytring og følelse av privatliv, noe også personvernkommisjonen

1 EMK Art. 6, pkt. 2

2 http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/

poengterte i sin utredning av DLD fra juni 2008[3]. Det er verdt å merke seg at selvsensur kan forekomme uansett lagringstid, hvem som har tilgang og under hvilke omstendigheter.

Lagringen vil ikke være sikker nok

Data kan og vil alltid bli misbrukt. Når så store mengder data skal ligge tilgjengelig i systemer er det ikke til å unngå at disse dataene vil bli offer for unødig uthenting og bruk. Det finnes rikelig med ferske eksempler på sensitiv informasjon som kommer på avveie til tross for streng lovgivning og sikkerhet. Deriblant har lister med personnummer[4], banktransaksjoner om kronprinsparet[5] og trafikkdata i offentlig sektor[6] kommet på avveie.

Det virker også svært sannsynlig at misbruken og menneskelig svikt vil være proporsjonal med mengden data, og her skiller masseinnsamling av data seg betraktelig fra direkte rettet etterforskning.

Dessverre er dette i hovedsak ikke et spørsmål om å øke sikkerheten på systemene for lagringen av disse dataene, men et overveiende problem gitt ved at dataene vil håndteres av svært mange mennesker. Antallet håndteringer vil være uavhengig av om dataene lagres i en sentral database eller hos de enkelte teletilbydere, selv om det siste nok vil være å foretrekke dersom DLD skulle bli innført i Norge.

Er det nødvendig?

Det har den siste tiden kommet uttalelser fra Politiet og Kripos hvor det gis et inntrykk av at man mangler de virkemidler som trengs for å etterforske alvorlig kriminalitet. Samtidig sitter man igjen med inntrykket av at DLD er den eneste løsningen på dette. Dette er et forvrengt bilde av virkeligheten.

Allerede i dag har Politiet tilgang på svært store mengder data som allerede finnes hos teletilbydere og som lagres der til praktiske formål. Politiet har mulighet til å hente ut disse dataene under etterforskning og eventuelt «fryse» dataene slik at de ikke slettes når det opprinnelige fristen for lagring i utgangspunktet er løpt ut. Det ligger i Politiets natur å alltid søke mer informasjon da deres rolle er å oppklare lovbrudd, men det er viktig at det er proporsjonalitet mellom gevinsten det gir for politiet og konsekvensene det medfører for den enkelte borger.

Hvis det er slik at Politiet i mange tilfeller opplever at helt kritiske data forsvinner før de har rukket å få de utlevert bør man i stedet se på dagens metoder og hjemler for uthenting av data. Det er trolig mange grunner til at slike tap forekommer, deriblant byråkratisk ventetid, men vi mener at det betyr at man trenger større ressurser til å behandle den informasjonen som allerede finnes heller enn at man øker mengden informasjon som samles inn.

Det finnes sikkert mangler i dagens systemer som kan utbedres før man går til en lettvint løsning som DLD, der man i stedet for å løse de konkrete problemene velger å skjære alle over en kam og glemmer det prinsipielle problemet ved å lagre trafikkdata for samtlige borgere.

Formålsglidning

Selv om det i høringsnotatet gjøres klart at kun Politiet skal få tilgang til dataene omfattet av DLD, er det tydelig av tidligere erfaringer og andre lands implementasjoner at DLD fort kan bli brukt til andre

3 http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/24.html?id=542291
4 http://www.nrk.no/nyheter/1.6222855
5 http://www.vg.no/nyheter/innenriks/kronprinsparet/artikkel.php?artid=164112
6 http://nrk.no/nyheter/1.6648860

formål enn hva det i utgangspunktet var tiltenkt.

En gjennomgang av DLDs forhold til sivile rettssaker gjort av advokat Jon Wessel-Aas viser klart at det med dagens lovgivning vil være hjemmel for bruk av disse dataene også i andre saker enn de som omfatter alvorlig kriminalitet[7].

Eksempler på saker hvor DLD kan komme til å finnes nyttig er barneomsorgssaker, trafikkforseelser, skatteunndragelse, opphavsrettsbrudd, mv. Dette er saker som hver for seg er viktige å håndheve, men satt i et system slik det DLD medfører, er et brudd med prinsippet om å ikke overvåke borgere uten skjellig grunn til mistanke og et steg bort fra et tillittsamfunn og inn i en kontrollstat.

Videre fremkommer det av høringsnotatet at det allerede i dag er et ønske om å utvide bruken av DLD til saker som går utover alvorlig kriminalitet med strafferammer over 3 år. Dette tyder på at velvilligheten til å bruke dataene til andre formål allerede er tilstede, og poengterer faren for at bruken av DLD kan utvides i fremtiden - enten gjennom politiske eller juridiske prosesser.

Strategisk informasjonsanalyse

DLD vil også øke potensialet for bruk av strategisk informasjonsanalyse (data-mining), hvor man ikke lenger går spesifikt inn etter direkte mistanke, men i stedet leter etter mønster som kan indikere avvik fra normalen. Det er velkjent innen læren om statistikk at man vil få svært mange falske positiver dersom man benytter identifikasjonssystemer med feilmarginer i store datamengder. Dette bør ses i sammenheng med at man i EU i dag nettopp jobber med å utvikle teknologi som skal samkjøre flere slike systemer som detekterer mistenkelig atferd. I Storbritannia er allerede flere slike systemer koblet sammen for å overvåke «Domestic Extremists» (personer assosiert med offentlige protester). Som et uheldig eksempel fra Storbritannia ble en mann registrert ved en protest mot andejakt i ettertid stoppet av politiet 25 ganger på 3 år. Dette skjedde hver gang analysesystemet oppfattet at mannen kjørte på en «mistenkelig» måte[8].

Opphavsrett

Åndsverksloven §54 gir anledning til å straffe forsettelig eller uaktsomt overtredelse av bestemmelser i nevnte lov med inntil tre måneder. Dette må bety at opphavsrettsbrudd ikke faller inn under bestemmelsene til DLD slik den foreligger i høringsnotatet. Høringsnotatet gir rom for unntak for minstebestemmelsen om tre års strafferamme, og vi vil understreke faren for fremtidig formålsglidning i forbindelse med brudd på åndsverkslovens bestemmelser. Dette er forankret i interesseorganisasjonene som representerer opphavsrettsindustriens sterke påvirkningskraft samt det sterke presset som legges av disse på lovgivende organ for å få utlevert trafikkdata.

Interesseorganisasjonene nevnt over har i dag sterk representasjon i departementets referansegruppe om ulovlig fildeling. I tillegg til dette er det gitt unntak fra taushetsplikten av Post- og teletilsynet i den sivile opphavsrettstvisten kjent som «Max Manus-saken». Denne avgjørelsen er for tiden til ankebehandling hos Høyesterett. Dette viser at selv med lovpålagt krav om taushetsplikt kan sterke interesser få gjennom krav om *legitim* utlevering av data, selv om det ligger utenfor det opprinnelige lagringsformålet.

7 http://www.uhuru.biz/?p=250

8 http://www.guardian.co.uk/uk/2009/oct/25/police-domestic-extremists-database

Konklusjon

Det enorme inngrepet av norske borgeres personvern som følge av en eventuell implementering av datalagringsdirektivet står i sterk kontrast til de udokumenterte og antatte positive egenskapene som proponentene har ytret. Faren for formålsglidning, altså at innsamlede data blir *legitimt* brukt til andre formål enn de ble lagret for, er overhengende. Bruk av lagrede trafikkdata som bevis i sivile rettsaker faller ikke inn under direktivets lagringsformål, men er et eksempel på lovlig bruk av trafikkdataene utover krav om minstestraff og er hjemlet i tvisteloven. I tillegg til dette er faren tilstede for at man utvider listen over lovbrudd utover det man i dag definerer som alvorlig kriminalitet, som hver for seg er viktig å håndheve, men som i verste fall kan føre oss et skritt nærmere en politistat.

Mye kan sies om de potensielle farene ved direktivet. Likevel bør det være tilstrekkelig å ta stilling til direktivets prinsipielle sider. Innføring av datalagringsdirektivet fører til en radikal forandring av rettsstaten hvor alle borgere mistenkeliggjøres og trafikkdata, bevegelsesmønster og kommunikasjonspartnere oppbevares med en *lagringsplikt* fra det som nå er en *sletteplikt*. Vi i FriBit ønsker ikke å leve i et samfunn hvor alle borgere overvåkes uten grunn til mistanke; derfor fraråder FriBit innlemmelsen av EUs datalagringsdirektiv i EØS-avtalen.

Med vennlig hilsen

FriBit

Svenn-Arne Dragly

Daglig leder